EMDOC
CONSORCIO

ITEM VI. PARTE A - PROPUESTA INFRAESTRUCTURA CENTRO DE DATOS

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

CONTENIDO

1. EQUIPOS ACTIVOS DE LA SOLUCIÓN PROPUESTA 3

1.1 DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA 3
1.1.1 Centro de Datos Principal 3
1.1.2 CENTRO DE DATOS ALTERNO 6
1.1.3 Licenciamiento Incluido 10
1.1.4 Mantenimiento y Soporte 10
1.2 DIAGRAMA DE LA SOLUCIÓN 11
1.2.1 Descripción 12

2. PLAN DE TRABAJO IMPLEMENTACIÓN INFRAESTRUCTURA EN CENTROS DE DATOS 14

2.1 ESTRUCTURA DEL PLAN DE TRABAJO 14
2.2 TAREAS Y ALCANCES 14
2.2.1 Tareas Generales 14
2.2.2 Tareas de Implementación e Instalación 15

3. JUSTIFICACIÓN 16

4. JUSTIFICACIÓN DEL PLAN DE RECUPERACIÓN Y RESPALDO 19

5. CAPACITACIÓN 21

5.1 VEEAM BACKUP AND REPLICATION 12.1 21
5.1.1 Objetivos de la Capacitación 22
5.1.2 Temario de la Capacitación 22
5.2 VMWARE VSPHERE: OPERATE, SCALE AND SECURE 23
5.2.1 Objetivos de la Capacitación 23
5.2.2 Temario de la Capacitación 24
5.3 HPE PROLIANT GEN11 SERVER MANAGEMENT WITH ILO 6 24
5.3.1 Objetivos de la Capacitación 25
5.3.2 Temario de la Capacitación 25

6. PREMISAS Y ENTREGABLES 26

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

EMDOC CONSORCIO

1. Equipos Activos de la Solución Propuesta

Nuestra propuesta incluye toda la infraestructura de hardware para soportar la solución de software para la impresión de la nueva cedula de identidad y electoral (CIE) y cedula de identidad (CI).

1.1 Descripción de la solución propuesta

La arquitectura está conformada por dos sitios que actuaran en configuración altamente disponible y redundante de cada uno; esto para garantizar la operación continua ante desastres o contingencias que se pudieran presentar. Nuestra propuesta incluye el equipamiento necesario para la operación de la solución propuesta, tanto para el sitio principal como para el alterno. A continuación, se detallan los componentes incluidos en nuestra oferta.

1.1.1 Centro de Datos Principal

Rack HPe 42U

Cantidad: uno (1)

Será utilizado para instalar los equipos activos de la solución propuesta. Incluye accesorios de fijación de este, así como PDUs de interconexión eléctrica de los equipos activos hasta la toma eléctrica suministrada por la JCE dentro del rack.

HPE Aruba Networking CX 6300M 24-port SFP+

Cantidad: dos (2)

Será utilizado para la interconexión de los elementos activos de la solución propuesta e integración a la red existente del cliente. Se requiere interconexión de los uplinks (mínimo cuatro por equipo) a cualquiera de las opciones soportadas (10/25/40/50/100 GbE) para la integración aguas arriba de la plataforma.

Fortinet FAD420F Balanceadores

Cantidad: dos (2)

Serán utilizados para balancear la carga para los servicios entrantes en los diferentes nodos de servicio de la infraestructura propuesta.

Hardware para la Plataforma PKI para grabado chip de cédulas - Servidores HPe Proliant DL380 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de PKI para grabado de chip de las cedulas, así como la infraestructura de administración de virtualización de la solución.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 256GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD

CONSORCIO EMDOC CONSORCIO Santo Domingo R.D.

- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma Mobile - Servidores HPe Proliant DL360 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de Mobile ID.
Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 384GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD
- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- 1 x tarjeta quad port 1Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Raiz)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad AC Raíz de la PKI Ciudadana.
Este servidor incluye:

- 1 x Procesadores Intel Xeon-S 4410Y 12 Cores a 2.0GHz
- 32GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Subordinadas)

Cantidad: dos (2)

Equipamiento activo que hospedará la entidad AC Subordinadas de la PKI Ciudadana.
Cada servidor incluye:

- 1 x Procesadores Intel Xeon-S 4416+ 20 Cores a 2.0GHz
- 64GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (Vertical de Firma)

Cantidad: dos (2)

Equipamiento activo que hospedará la entidad Vertical de Firmas de la PKI Ciudadana.
Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz

- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (SeguriSign, SeguriNotary, OCSP)

Cantidad: dos (2)

Equipamiento activo que hospedará la entidad SeguriSign, SeguriNotary y OCSP de la PKI Ciudadana.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz
- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para Aplicaciones (POC)- Servidores HPe Proliant DL20 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la de POC de los componentes DB, APP, Auth de los servicios.

Este servidor incluye:

- 1 x Procesadores Intel Xeon E-2468 8 Cores a 2.6GHz
- 64GB de RAM
- 2 x HPE 1TB HDD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros

Hardware para Aplicaciones (Ambiente Redundante)- Servidores HPe Proliant DL380 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de Mobile ID.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 5418Y 24 Cores a 2.0GHz
- 256GB de RAM
- 4 x HPE 480GB SATA RI SFF BC MV SSD
- 4 x HPE 1.6TB SATA RI SFF BC MV SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Appliance de Backup HPe StoreOnce 3660

Cantidad: uno (1)

Solución de respaldo para realizar las copias de seguridad necesarios para garantizar la operación ante desastres de la arquitectura propuesta.

Incluye capacidad de backup para 96TB

Unidad de Almacenamiento HPE MSA 2062 10GbE iSCSI

Cantidad: uno (1)

Será utilizado como unidad de almacenamiento de toda la infraestructura para proveer servicios de datos estructurados y no estructurados a la plataforma.

Incluye:

- 16 x HPE MSA 3.84TB SAS RI SFF M2 SSD
- 4 x Puertos 10Gbs

Hardware para Backup y Proxy VEEAM - Servidores HPe Proliant modelos DL360 Gen11

Cantidad: dos (2)

Equipamiento activo para la administración de la solución de backup y realización de estos a través de agentes y/o funciones nativas de la plataforma de virtualización.

Cada servidor incluye:

- 1x Procesador Intel Intel Xeon Gold 5416S 2.0GHz
- 32GB de RAM
- 2x HPE 960GB SATA RI SFF BC MV SSD
- 1 x tarjeta doble port 1Gbps
- 1 x tarjeta doble port 10Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Módulos criptográficos

- 1 Utimaco CryptoServer CP5 Se52PCIe, CC certified acc. EN419221-5
- 1 Utimaco CC eIDAS on CryptoServer General Purpose Network HSM SecurityServer Se100 LAN V5
- Se incluyen también 10 Fichas criptográficas USB (material de claves y certificados de autenticación de clientes), para el equipo de administrac
- 2 módulos de seguridad criptográfica CryptoServer CP5 Se 500 de Utimaco, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 2 equipos serán para ambiente productivo y 1 equipo para ambiente DRP.
- 1 módulos de seguridad criptográfica CryptoServer CP5 Se 12, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 1 equipo será para ambiente productivo y 1 equipo para ambiente DRP.

1.1.2 CENTRO DE DATOS ALTERNO

Rack HPe 42U

Cantidad: uno (1)

Será utilizado para instalar los equipos activos de la solución propuesta. Incluye accesorios de fijación de este, así como PDUs de interconexión eléctrica de los equipos activos hasta la toma eléctrica suministrada por la JCE dentro del rack.

HPE Aruba Networking CX 6300M 24-port SFP+

Cantidad: dos (2)

Será utilizado para la interconexión de los elementos activos de la solución propuesta e integración a la red existente del cliente. Se requiere interconexión de los uplinks (mínimo cuatro por equipo) a cualquiera de las opciones soportadas (10/25/40/50/100 GbE) para la integración aguas arriba de la plataforma.

Fortinet FAD420F Balanceadores

Cantidad: dos (2)

Serán utilizados para balancear la carga para los servicios entrantes en los diferentes nodos de servicio de la infraestructura propuesta.

Hardware para la Plataforma PKI para grabado chip de cédulas - Servidores HPe Proliant DL380 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de PKI para grabado de chip de las cedulas, así como la infraestructura de administración de virtualización de la solución.
Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 256GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD
- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma Mobile - Servidores HPe Proliant DL360 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la solución de Mobile ID.
Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 384GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD
- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- 1 x tarjeta quad port 1Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Raiz)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad AC Raíz de la PKI Ciudadana.
Este servidor incluye:

- 1 x Procesadores Intel Xeon-S 4410Y 12 Cores a 2.0GHz

- 32GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Subordinadas)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad AC Subordinadas de la PKI Ciudadana.

Este servidor incluye:

- 1 x Procesadores Intel Xeon-S 4416+ 20 Cores a 2.0GHz
- 64GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (Vertical de Firma)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad Vertical de Firmas de la PKI Ciudadana.

Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz
- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (SeguriSign, SeguriNotary, OCSP)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad SeguriSign, SeguriNotary y OCSP de la PKI Ciudadana.

Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz
- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para Aplicaciones (POC)- Servidores HPe Proliant DL20 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la de POC de los componentes DB, APP, Auth de los servicios.

Este servidor incluye:

- 1 x Procesadores Intel Xeon E-2468 8 Cores a 2.6GHz
- 64GB de RAM

- 2 x HPE 1TB HDD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros

Hardware para Aplicaciones (Ambiente Redundante)- Servidores HPe Proliant DL380 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la solución de Mobile ID.
Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 5418Y 24 Cores a 2.0GHz
- 256GB de RAM
- 4 x HPE 480GB SATA RI SFF BC MV SSD
- 4 x HPE 1.6TB SATA RI SFF BC MV SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Appliance de Backup HPe StoreOnce 3660

Cantidad: uno (1)

Solución de respaldo para realizar las copias de seguridad necesarios para garantizar la operación ante desastres de la arquitectura propuesta.
Incluye capacidad de backup para 96TB

Unidad de Almacenamiento HPE MSA 2062 10GbE iSCSI

Cantidad: uno (1)

Será utilizado como unidad de almacenamiento de toda la infraestructura para proveer servicios de datos estructurados y no estructurados a la plataforma.
Incluye:

- 16 x HPE MSA 3.84TB SAS RI SFF M2 SSD
- 4 x Puertos 10Gbs

Hardware para Backup y Proxy VEEAM - Servidores HPe Proliant modelos DL360 Gen11

Cantidad: dos (2)

Equipamiento activo para la administración de la solución de backup y realización de estos a través de agentes y/o funciones nativas de la plataforma de virtualización.
Cada servidor incluye:

- 1x Procesador Intel Intel Xeon Gold 5416S 2.0GHz
- 32GB de RAM
- 2x HPE 960GB SATA RI SFF BC MV SSD
- 1 x tarjeta doble port 1Gbps
- 1 x tarjeta doble port 10Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Módulos criptográficos

- 1 Utimaco CryptoServer CP5 Se52PCIe, CC certified acc. EN419221-5

- 1 Utimaco CC eIDAS on CryptoServer General Purpose Network HSM SecurityServer Se100 LAN V5
- Se incluyen también 10 Fichas criptográficas USB (material de claves y certificados de autenticación de clientes), para el equipo de administrac
- 1 módulos de seguridad criptográfica CryptoServer CP5 Se 500 de Utimaco, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 2 equipos serán para ambiente productivo y 1 equipo para ambiente DRP.
- 1 módulos de seguridad criptográfica CryptoServer CP5 Se 12, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 1 equipo será para ambiente productivo y 1 equipo para ambiente DRP.

En este caso, la JCE es responsable de suministrar el espacio requerido para la instalación del rack que hospedará todos los equipos activos de la solución tanto en el centro de datos primario, como en el secundario. En adición, es responsable de garantizar la conectividad eléctrica y de datos requerida para la correcta operación de la solución.

1.1.3 Licenciamiento Incluido

Se incluye el siguiente licenciamiento para todos los equipos

- Red Hat Enterprise Linux Server, Premium (Physical or Virtual Nodes)
- vMware Standard
- Veeam Data Platform Premium. 3 Years Subscription Upfront Billing & Production (24/7) Support. Public Sector
- PostgreSQL Database

Nota: Todos los softwares incluidos son de tipo suscripción por treinta y seis (36) meses.

1.1.4 Mantenimiento y Soporte

Nuestra propuesta incluye soporte y garantías directo del fabricante según lo siguiente:

Garantía

- El hardware incluye garantía de hardware del fabricante por sesenta (60) meses con reemplazo de partes y almacén de piezas local.
- El Consorcio EMDOC brindará el servicio de reemplazo de partes una vez estas sean entregadas por el fabricante en las instalaciones de la JCE.

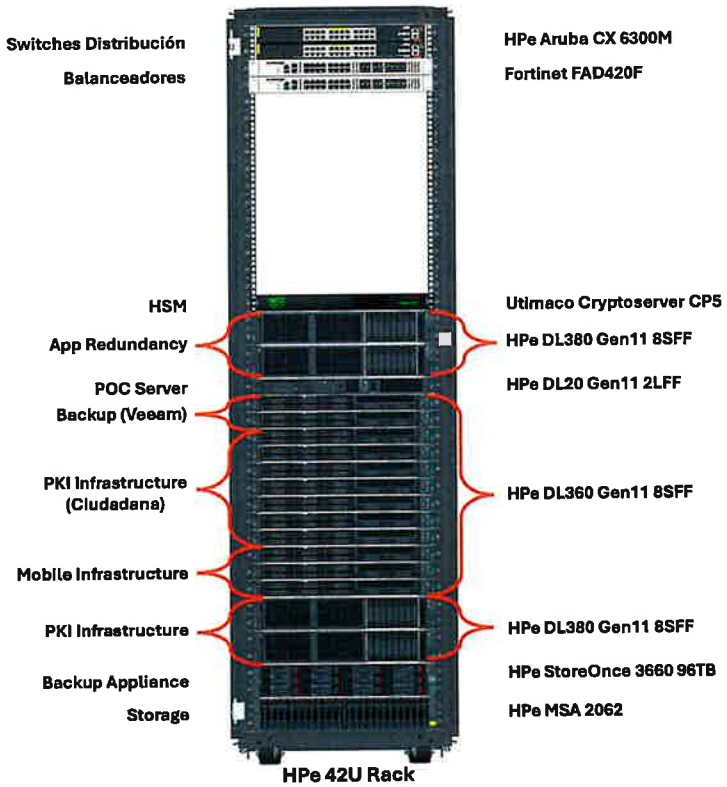
Soporte

- Se incluye soporte para el hardware, sistemas operativos y base de datos por (60) meses con SLA 7x24x365.
- El soporte incluye atención nivel 1 y 2 por parte del Consorcio EMDOC. El soporte nivel 3 será brindado por el fabricante.

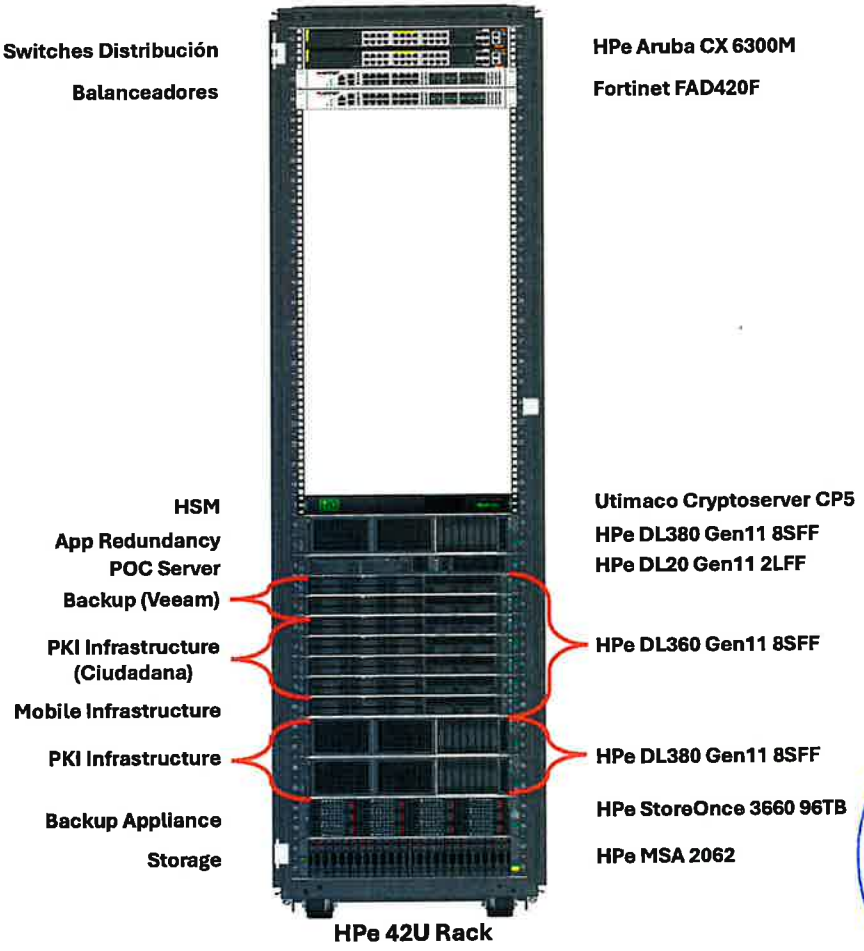
- El Consorcio EMDOC estará realizando visitas bianuales para el correcto mantenimiento preventivo de la infraestructura propuesta. Este mantenimiento preventivo incluye:
  - Monitoreo de temperatura y consumo eléctrico.
  - Detección de fallos en componentes internos (discos, memorias, tarjetas).
  - Revisión de logs de eventos críticos.
  - Verificación de alertas en los sistemas de gestión/administración.
  - Revisión de firmware (BIOS, controladoras, tarjetas de red).
  - Evaluación de consumo de recursos (CPU, RAM, discos).
  - Verificación de snapshots y replicación de datos.
  - Evaluación de la capacidad utilizada y planificación de expansión.
  - Aplicación de parches de seguridad y actualizaciones menores.
  - Verificación de servicios críticos en ejecución.

1.2 Diagrama de la Solución

La solución está compuesta por dos gabinetes instalado en cada uno de los centros de datos, primario y secundario de la JCE.
En el caso del Centro de Datos Primario se tiene:



Para el Centro de Datos Primario se estará consumiendo un total de 30 unidades de rack, quedando libres unas 12 unidades de rack que podrán ser utilizadas para futuro crecimiento y expansión de la plataforma.
En el caso del Centro de Datos Secundario se tiene:



Para el Centro de Datos Primario se estará consumiendo un total de 24 unidades de rack, quedando libres unas 18 unidades de rack que podrán ser utilizadas para futuro crecimiento y expansión de la plataforma.

1.2.1 Descripción

Se contará con un rack HPe de 42U en cada localidad. El Rack HPe 42U permitirá contar con una infraestructura tecnológica de alta disponibilidad diseñada para optimizar la gestión de redes, aplicaciones, seguridad y almacenamiento de datos en entornos empresariales y gubernamentales. Está compuesto por equipos de última generación que garantizan rendimiento, seguridad y escalabilidad.

HPe Aruba CX 6300M (Switch de Distribución)
Switch de red de alto rendimiento diseñado para la distribución eficiente del tráfico.
Beneficios: Proporciona conectividad rápida y confiable con capacidades avanzadas de automatización y administración.
Seguridad: Soporte para políticas de acceso, segmentación de tráfico y protección contra ataques de red.
Redundancia: Capacidad de stacking y enlaces redundantes para evitar fallos en la red.

Fortinet FAD420F (Balanceador de Carga)
Dispositivo de balanceo de carga para distribuir tráfico entre servidores y mejorar la disponibilidad de servicios.
Beneficios: Optimiza el rendimiento, mejora la experiencia del usuario y reduce el tiempo de inactividad.
Seguridad: Protección contra ataques DDoS y control de tráfico cifrado.
Redundancia: Distribución inteligente del tráfico para evitar sobrecargas en servidores críticos.

Utimaco Cryptoserver CP5 (HSM – Hardware Security Module)
Módulo de seguridad que protege claves criptográficas y gestiona procesos de cifrado.
Beneficios: Garantiza la seguridad de firmas digitales, certificados y cifrado de datos sensibles.
Seguridad: Certificado bajo estándares internacionales como FIPS 140-2, asegurando máxima protección.
Redundancia: Configuración en clúster para asegurar disponibilidad continua de claves criptográficas.

Ambiente de KPI para grabado de chip de cédulas
Formado por un clúster en alta disponibilidad con componentes físicos y virtuales. Los cuales estarán compuestos por servidores redundantes.

Ambiente de KPI Ciudadana
Formado por un clúster en alta disponibilidad con componentes físicos y virtuales. Los cuales estarán compuestos por servidores redundantes:

- PKI
- ACC RAIZ
- AC Subordinada
- Vertical de Firma
- SeguriSign, SeguriNotary, OCSP (Cloud)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

Ambiente de Mobile ID
Formado por un clúster virtualizado formado por tres servidores en un ambiente totalmente en HA. Los cuales estarán compuestos por servidores virtuales redundantes:

- Database Server
- Authentication Server
- Application Server

Replicación y Orquestación

Para la replicación y orquestación del Site principal al Site alterno se incluye el licenciamiento de VEEAM Backup and Replicator en su versión Premium.

	Base Fundación segura	Avanzado Ciberresiliencia	De primera calidad Resiliencia empresarial
	✓ Copia de seguridad y recuperación	✓ Copia de seguridad y recuperación ✓ Monitoreo y análisis	✓ Copia de seguridad y recuperación ✓ Monitoreo y análisis ✓ Orquestación de recuperación
+ Protección para hipervisores, nubes y aplicaciones líderes en la industria	●	●	●
+ Portabilidad de datos para una flexibilidad total sin ataduras	●	●	●
+ Asistencia y remediación impulsadas por IA	◐	●	●
+ Refuerce sus datos de respaldo con la detección de amenazas durante el ciclo de vida	◐	◔	●
+ Arquitectura de resiliencia de datos de confianza cero	◐	◔	●
+ Integración perfecta con herramientas de seguridad y flujos de trabajo	◐	◔	●
+ Análisis y generación de informes sólidos	○	◔	●
+ Información detallada sobre su gobernanza y cumplimiento	◐	◔	●
+ Pruebas de recuperación automatizadas inigualables	◐	◐	●
+ Recuperación de datos confiable, escalable y orquestada	○	○	●

2. Plan de Trabajo Implementación Infraestructura en Centros de Datos

Este documento establece el plan de trabajo detallado para el proyecto del CLIENTE. El objetivo principal es actualizar y fortalecer la infraestructura tecnológica para mejorar la eficiencia operativa y garantizar un proceso de implementación, según las mejores prácticas del fabricante entregado por personal debidamente calificado y certificado.

2.1 Estructura del Plan de Trabajo

El proyecto se divide en varias fases, cada una con tareas y subtareas. Los recursos, las duraciones, las dependencias y las fechas de inicio y finalización se deben introducir en Microsoft Project.

2.2 Tareas y Alcances

Se incluyen los servicios de instalación e implementación de toda la solución propuesta.

2.2.1 Tareas Generales

- ✓ Nuestra propuesta incluye la asignación de un gerente de proyectos certificado PMP dedicado 100% de su tiempo a la implantación de todas las soluciones ofertadas hasta la conclusión y recepción del proyecto.

- ✓ Nuestra propuesta incluye plan de trabajo detallado en el cual se especifica de forma clara todos los pasos a ejecutar durante el proceso de implementación de la solución ofertada.
- ✓ Ejecución de pruebas.
- ✓ Documentación completa del proyecto.
- ✓ Capacitación del proceso de implementación.

2.2.2 Tareas de Implementación e Instalación

Servicio de implementación para el almacenamiento

- ✓ Instalación física del equipo
- ✓ Cableado del equipo
- ✓ Startup y configuración
- ✓ Actualización de versión de BIOS FIRMWARE y OS
- ✓ Creación de Raid Group y Volúmenes
- ✓ Pruebas de lectura y escritura

Tareas implementación Servidores

- ✓ Validación de Prerrequisitos de instalación
- ✓ Instalación física de servidores
- ✓ Configuración de out-of-band mgmt (iDRAC, CIMC, iLO, IMM, etc), arreglo de discos locales y políticas de BIOS.
- ✓ Instalación de sistema operativo.
- ✓ Ejecución de pruebas

Servicio de implementación Switches

- ✓ Validación de Prerrequisitos de instalación, incluyendo JCE
- ✓ Instalación de los Switches en Rack
- ✓ Encendido y Actualización de versión de UCSM, BIOS y Firmware
- ✓ Configuración de management y cluster
- ✓ Configuración de puertos para servidores
- ✓ Configuración de puertos y uplinks
- ✓ Integración a ambiente actual

Servicio de implementación VEEAM

- ✓ Validación de prerrequisitos de instalación
- ✓ Instalación y configuración básica VEEAM Backup
- ✓ Creación de Jobs de respaldo y Jobs de replicación

Servicio de implementación VMware

- ✓ Validación de Prerrequisitos de instalación, incluyendo JCE
- ✓ Instalación y configuración vCenter
- ✓ Instalación y configuración eSXI

Servicio de implementación Appliance Backup

- ✓ Validación de Prerrequisitos de instalación incluyendo JCE

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- ✓ Instalación física del Appliance
- ✓ Configuración de networking
- ✓ Inicialización y configuración
- ✓ Configuración de proxy
- ✓ Pruebas de Backup/Respaldo

Consideraciones para el servicio

- ✓ La JCE debe proporcionar un área de trabajo adecuada para la entrega del servicio, incluido el acceso a una línea telefónica externa, energía y cualquier conexión de red requerida.
- ✓ La JCE debe permitir al Consorcio EMDOC acceso total y sin restricciones a todas las ubicaciones donde se realizará el servicio.

Premisas

- ✓ La capacidad del Consorcio EMDOC para brindar los servicios depende de la cooperación total y oportuna de la JCE con el Consorcio EMDOC, así como de la precisión e integridad de cualquier información y datos que la JCE proporcione al Consorcio EMDOC.
- ✓ Se incluyen en el proceso de entrega de los servicios varios recursos técnicos los cuales realizan la entrega de servicios en paralelo.
- ✓ La entrega programada de servicios se coordina entre el gerente de proyecto del Consorcio EMDOC y la JCE.

Entregables

- ✓ Capacitación.
- ✓ Documentación completa del proyecto.
- ✓ Pruebas funcionales y operativas.
- ✓ Reporte de certificación de trabajos concluidos, el cual incluye imágenes de los equipos ya instalados, y la confirmación de la puesta en servicio de la solución y/o equipo instalado.
- ✓ Certificación al final del proceso de implementación de que la misma fue realizada según las mejores prácticas y en cumplimientos de versiones de software recomendados al momento de la implementación.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

3. Justificación

3.1. Los equipos del Ambiente Productivo de la PKI y DRP se justifican de la siguiente manera:

SeguriServer (AC Raíz):

Recurso	Justificación
Procesador	La AC raíz ejecutará tareas críticas como la firma de certificados subordinados y listas de revocación (CRL). Un procesador con 10 núcleos es suficiente, ya que esta CA opera en un entorno aislado con baja carga transaccional, sin embargo, se conectará al

	Cryptoserver CP5 SE12, por lo cual requiere esta capacidad de procesamiento.
Memoria RAM	Se requiere una cantidad de RAM adecuada para ejecutar Windows Server 2022, gestionar firmas digitales y realizar auditorías de seguridad sin degradar el rendimiento.
Almacenamiento	Se utiliza almacenamiento NVMe SSD por su velocidad y confiabilidad. Dado que la AC raíz solo firmará certificados en momentos específicos y la base de datos estará en un servidor externo, este espacio es suficiente para el sistema operativo, software PKI y logs de auditoría.
Sistema Operativo	Compatible con los requisitos de PKI, HSM UTIMACO y cumple con los lineamientos de seguridad y compatibilidad requeridos para la infraestructura.

SeguriServer (AC Ruiz)

Recurso	Justificación
Procesador	Se requiere un CPU con alto rendimiento en procesamiento paralelo para manejar la carga computacional de la generación y validación de claves criptográficas, firmas digitales y operaciones de cifrado/descifrado. Un procesador con múltiples núcleos permite optimizar la concurrencia de procesos y minimizar la latencia, lo que es fundamental al momento de crear los certificados de la PKI ciudadana. Adicionalmente, este servidor estará conectado al Cryptoserver CP5 SE 500, por lo cual requiere un mayor procesamiento para comunicarse de manera efectiva con el mismo.
Memoria RAM	La PKI debe manejar múltiples peticiones simultáneas, desde la emisión de certificados hasta su validación en tiempo real. Además, el entorno requiere ejecución eficiente de servicios de autenticación y cifrado, minimizando el riesgo de degradación del rendimiento.
Almacenamiento	Se opta por almacenamiento NVMe SSD debido a su velocidad de lectura/escritura superior, lo que mejora el tiempo de respuesta del sistema. Este espacio cubre el sistema operativo, aplicaciones y logs de auditoría. La base de datos de certificados se alojará en un servidor externo, optimizando la distribución de carga.
Sistema Operativo	Compatible con los requisitos de PKI y cumple con los lineamientos de seguridad y compatibilidad requeridos para la infraestructura.
	Portal de Firma
Recurso	Justificación
Procesador	Se requiere un procesador de alto rendimiento con múltiples núcleos para manejar la concurrencia de solicitudes en el portal y la ejecución de microservicios en Java. Los procesos de firma digital y cifrado demandan potencia computacional significativa, especialmente en cargas transaccionales altas.

Memoria RAM	Los microservicios en Java tienden a un alto consumo de memoria debido a la administración de sesiones, el manejo de documentos y las validaciones criptográficas. Se requiere suficiente RAM para evitar cuellos de botella y garantizar tiempos de respuesta óptimos.
Almacenamiento	Se opta por almacenamiento NVMe SSD debido a su velocidad superior, lo que reduce la latencia en la ejecución de servicios y el acceso a logs. Aunque la base de datos es externa, este espacio es necesario para almacenar logs de auditoría, archivos temporales y procesamiento de documentos.
Sistema Operativo	Se requiere un sistema operativo estable y seguro que sea compatible con Java, Apache Tomcat y la infraestructura de microservicios, garantizando compatibilidad con entornos empresariales.
	SeguriSign, SeguriNotary, OCSP
Recurso	Justificación
Procesador	Se requiere un procesador de alto rendimiento para gestionar múltiples solicitudes concurrentes de firma, validación y estampillado en tiempo real. Cada operación criptográfica consume recursos intensivos de CPU, especialmente en volúmenes altos de transacciones.
Memoria RAM	Los servicios de firma, TSA y OCSP requieren gestión eficiente de memoria, ya que manejan múltiples sesiones simultáneamente. Los microservicios en Java y los servidores Tomcat también incrementan el consumo de memoria.
Almacenamiento	Se utiliza almacenamiento NVMe SSD debido a su velocidad y confiabilidad. Aunque la base de datos es externa, este espacio es necesario para logs de auditoría, transacciones temporales y caché de validación OCSP.
Sistema Operativo	Se requiere un sistema operativo estable y seguro que sea compatible con Java, Apache Tomcat y la infraestructura de microservicios, garantizando compatibilidad con entornos empresariales.
	Base de Datos
Recurso	Justificación
Procesador	Se requiere una CPU de alto rendimiento debido al procesamiento intensivo de consultas, índices y transacciones. La base de datos manejará operaciones criptográficas, validaciones y logs de auditoría de los servicios core.
Memoria RAM	SQL Server realiza almacenamiento en caché de consultas y datos en memoria para optimizar tiempos de respuesta. Se requiere esta capacidad para soportar la carga transaccional y minimizar el acceso a disco.
Almacenamiento	Se utiliza NVMe SSD para garantizar tiempos de acceso ultra rápidos, minimizando la latencia en la escritura y lectura de datos. Se estima un almacenamiento eficiente para 4,000,000 de

	documentos en dos años, esto debido a la emisión de 800,000 certificados para ciudadanos y un promedio de 5 firmas de documentos por ciudadano. Tomando como consideración un peso promedio por PDF de 1.7 MB y un promedio de dos firmas por documento, queda un tamaño final de 2 MB por documento concluido. Tomando en consideración lo anterior, bajo el supuesto de que cada usuario firma 5 documentos por año, se tiene que en dos años se firmarán 4,000,000 de documentos multiplicado por los 2 MB, da un total de 8TB para la base de firma, a esto se debe aumentar las otras bases que utiliza la plataforma de firma y que, en promedio, por dos años medirán de 1 TB.
Sistema Operativo	Garantiza compatibilidad total con SQL Server 2022, con soporte para configuraciones avanzadas de clúster y alta disponibilidad.

4. Justificación del Plan de Recuperación y Respaldo

El Consorcio EMDOC con la finalidad de garantizar la continuidad del negocio y la recuperación ante desastres de la infraestructura PKI, propone el siguiente implementación de un plan integral de Disaster Recovery Plan (DRP) alineado con estándares internacionales como la ISO/IEC 27031, que establece directrices para la preparación en tecnologías de la información, y la ISO 22301, enfocada en sistemas de gestión de continuidad del negocio. Este plan no solo asegura el cumplimiento normativo, sino que también prioriza la disponibilidad y protección de los servicios críticos y la información sensible alojada en el Centro de Datos.

Como herramienta clave para la ejecución efectiva de este plan, estaremos utilizando Veeam Backup and Replication en su versión Premium. Esta solución permite gestionar de manera eficiente los respaldos y la replicación de datos, asegurando una recuperación rápida y confiable (Recovery Time Objective - RTO) ante incidentes que afecten la infraestructura o los servicios de la PKI. Veeam Backup and Replication Premium ofrece funcionalidades avanzadas para proteger, mitigar y gestionar riesgos y amenazas, ya sean de origen físico, lógico o por error humano. Entre sus capacidades destacan:

- **Respaldo y replicación automatizados**: Garantiza la integridad y disponibilidad de la información crítica mediante copias de seguridad consistentes y réplicas en tiempo real de los sistemas PKI.
- **Soporte Específico para Bases de Datos PostgreSQL y Microsoft SQL Server.** La capacidad de Veeam para manejar estas bases de datos asegura que los servicios críticos dependientes (como PKI, firma ciudadana y Mobile ID) puedan recuperarse de manera ordenada y funcional, respetando las mejores prácticas de la industria.
- **Recuperación granular y rápida**: Permite restaurar servicios o datos específicos en minutos, minimizando el impacto en las operaciones.
- **Gestión centralizada**: Facilita la administración de respaldos y réplicas, asegurando una visión integral de la infraestructura crítica.

- **Pruebas de recuperación**: Ofrece la posibilidad de simular escenarios de desastre sin afectar los entornos productivos, validando la efectividad del DRP.
- **Cumplimiento de políticas de continuidad**: Asegura que los tiempos de recuperación y la disponibilidad de datos cumplan con los objetivos estratégicos de la empresa.

Con Veeam Backup and Replication Premium, la empresa podrá proteger su infraestructura PKI frente a interrupciones no planificadas, garantizando la continuidad del negocio y la disponibilidad de servicios esenciales. Esta solución, combinada con un DRP bien estructurado, proporciona una respuesta proactiva y robusta ante cualquier eventualidad, salvaguardando tanto la operatividad como la información vital para el cumplimiento de los objetivos organizacionales.

Abordaje para recuperación ante desastres

A continuación, se detalla el enfoque recomendado para la recuperación manual (basado en recomendaciones de la industria y mejores prácticas), respetando el orden de encendido establecido:

1. Bases de datos, ambientes virtuales y aplicaciones secundarias:
a. Se iniciará la restauración manual de las bases de datos críticas, esenciales para el funcionamiento de los sistemas, utilizando las funcionalidades de recuperación granular de Veeam. Esto asegura que los datos estén disponibles antes de proceder con otros componentes.
b. Posteriormente, se restaurarán los ambientes virtuales que soportan estas bases y las aplicaciones secundarias, verificando su integridad y conectividad paso a paso, conforme a las mejores prácticas de recuperación de entornos virtualizados.
2. Ambiente PKI:
a. Una vez confirmado el funcionamiento de las bases de datos y los ambientes virtuales, se procederá con la recuperación manual del ambiente PKI. Veeam permite restaurar las máquinas y configuraciones específicas de este entorno, asegurando que los servicios de infraestructura de clave pública estén operativos antes de avanzar al siguiente nivel.
3. Ambiente de firma ciudadana y Mobile ID:
a. Finalmente, se restaurará el ambiente de firma ciudadana y Mobile ID, que depende de la disponibilidad previa del PKI y las aplicaciones secundarias. Este paso se ejecutará manualmente, validando cada componente para garantizar la continuidad de los servicios ciudadanos sin interrupciones.

Cabe destacar que se recomienda a la JCE realizar ejercicios de recuperación ante desastres para garantizar la ejecución optima de procesos y controles que garantizan una correcta operación luego del desastre en el sitio secundario. Estos ejercicios deben ser realizados por la JCE, con el apoyo del personal del Consorcio EMDOC.

Recomendaciones para el Plan de Recuperación Ante Desastres

Basado en las normativas ISO/IEC 27031 (directrices para la preparación en tecnologías de la información) e ISO 22301 (sistemas de gestión de continuidad del negocio), las recomendaciones para los parámetros de RPO (Recovery Point Objective), RTO (Recovery Time Objective) y las pruebas dependen de la criticidad de los sistemas y

servicios involucrados, como la infraestructura PKI, las bases de datos, y los ambientes de firma ciudadana y Mobile ID. A continuación, se detallan las recomendaciones generales alineadas con estas normativas y adaptadas al contexto la plataforma ofertada, considerando las mejores prácticas de la industria y el uso de Veeam Backup and Replication Premium:

Componente	RPO Recomendado	RTO Recomendado	Frecuencia de Pruebas
Bases de datos y ambientes virtuales	15 min - 1 hora	1 - 4 horas	Trimestral + Anual
Ambiente PKI	15 min - 1 hora	4 - 8 horas	Trimestral + Anual
Firma ciudadana y Mobile ID	15 min - 1 hora	8 - 12 horas	Trimestral + Anual

Veeam Backup and Replication Premium ofrece una solución integral que satisface las necesidades técnicas y normativas de la JCE:

- Soporte avanzado para PostgreSQL y Microsoft SQL Server
- Flexibilidad para una recuperación manual ordenada
- Cumplimiento de RPO y RTO objetivos (15 min-1 hora y 1-12 horas, respectivamente)
- Capacidades de prueba robustas.

Protege la infraestructura crítica de la PKI y sus servicios asociados, asegurando la continuidad del negocio frente a cualquier incidente, mientras se alinea con las mejores prácticas y las normativas ISO/IEC 27031 e ISO 22301. Es una herramienta probada que combina eficacia, control y confiabilidad, lo que la convierte en la opción ideal para este caso.

5. Capacitación

Como parte de los entregables, se estarán realizando capacitaciones con el personal del Consorcio EMDOC en los que se habilitará a los ingenieros de la JCE en la correcta operación, mantenimiento y monitoreo de la infraestructura propuesta. A continuación se detallan estas capacitaciones:

5.1 Veeam Backup and Replication 12.1

La capacitación sobre Veeam Backup & Replication v12.1: Configuración, Gestión y Recuperación está diseñada para brindar a los participantes los conocimientos y habilidades necesarios para administrar y optimizar soluciones de respaldo y recuperación de datos utilizando Veeam. La capacitación se centra en la protección de datos en entornos físicos y virtuales desplegados en la JCE, incluyendo estrategias de seguridad, optimización del almacenamiento y recuperación ante desastres.

Metodología

El curso sigue una metodología teórico con ejemplos prácticos de lo implementado. Se utilizarán los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicaciones sobre cada tema clave.
- ✓ Ejemplos prácticos: Guía y muestra en vivo de la herramienta para reforzar conceptos basado en la configuración implementada.
- ✓ Preguntas y respuestas: Espacios interactivos para resolver dudas.
- ✓ Duración: dos (2) días.

Incluye:

- ✓ Conceptos clave de seguridad en Veeam.
- ✓ Visualización de la configuración y optimización de backups y réplicas.
- ✓ Gestión del almacenamiento y estrategias de recuperación.
- ✓ Pruebas de recuperación y validación de integridad.
- ✓ Escenarios prácticos con resolución de problemas.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

No Incluye:

- ✓ Implementaciones personalizadas.
- ✓ Configuración avanzada fuera del entorno estándar del curso.
- ✓ Material oficial, libros y/o guías de certificación.
- ✓ Refrigerio.
- ✓ Certificación oficial del fabricante.

5.1.1 Objetivos de la Capacitación

Al finalizar la capacitación, los participantes podrán:

1. Comprender las estrategias de protección de datos y mitigación de riesgos.
2. Configurar y gestionar trabajos de backup y copia de seguridad.
3. Implementar medidas de seguridad para proteger la infraestructura de respaldo.
4. Optimizar el almacenamiento mediante técnicas avanzadas de Veeam.
5. Restaurar datos utilizando diferentes métodos de recuperación.
6. Integrar Veeam en planes de respuesta ante incidentes.

5.1.2 Temario de la Capacitación

1. Introducción a la Protección de Datos
   - Importancia del respaldo y recuperación.
   - Estrategias clave de protección de datos.
2. Componentes Clave de Veeam Backup & Replication
   - Infraestructura básica.
   - Requisitos del sistema.
3. Visualización de configuración Inicial y Seguridad
   - Visualización de configuración del servidor de backup.
   - Medidas de seguridad para evitar accesos no autorizados.
4. Creación y Gestión de Backups
   - Respaldo de máquinas virtuales (VMware y Hyper-V).
   - Protección de datos no estructurados y agentes de backup.
5. Optimización del Almacenamiento y Retención
   - Técnicas de optimización de datos.
   - Repositorios de backup y almacenamiento en la nube.

6. Replicación y Alta Disponibilidad
   - Configuración de trabajos de replicación.
   - Protección continua de datos (CDP).
7. Recuperación de Datos y Planificación ante Incidentes
   - Métodos de recuperación según escenarios.
   - Integración de Veeam en planes de respuesta ante incidentes.

5.2 VMware vSphere: Operate, Scale and Secure

La capacitación VMware vSphere: Operate, Scale and Secure [V8] está diseñada para brindar conocimiento en la gestión avanzada de VMware vSphere 8. Se enfoca en la configuración, escalabilidad y seguridad de entornos virtualizados, cubriendo desde la administración de redes y almacenamiento hasta la protección y recuperación de máquinas virtuales.

Metodología
Esta capacitación tiene un enfoque teórico con ejemplos prácticos. Se utilizarán los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicación de conceptos clave y mejores prácticas.
- ✓ Ejemplos prácticos: Guía y muestra en vivo en el ambiente real de VMware vSphere para reforzar el aprendizaje.
- ✓ Espacios de preguntas y respuestas: Interacción para aclarar dudas.
- ✓ Duración: dos (2) días.

Incluye:

- ✓ Conceptos clave de VMware vSphere 8.
- ✓ Gestión de seguridad, acceso y monitoreo de entornos virtualizados.
- ✓ Administración de alta disponibilidad y recuperación de máquinas virtuales.
- ✓ Estrategias de escalabilidad y optimización del rendimiento.
- ✓ Escenarios prácticos con resolución de problemas.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

No Incluye:

- ✓ Implementaciones personalizadas.
- ✓ Configuración avanzada fuera del entorno estándar del curso.
- ✓ Material oficial, libros y/o guías de certificación.
- ✓ Refrigerio.
- ✓ Certificación oficial del fabricante.

5.2.1 Objetivos de la Capacitación

Al finalizar la capacitación, los participantes podrán:

1. Administrar un VMware Tools Repository.

2. Operar vSphere Replication y recuperar máquinas virtuales replicadas.
3. Gestionar recursos de máquinas virtuales mediante Resource Pools.
4. Administrar redes y almacenamiento para entornos empresariales complejos.
5. Implementar alta disponibilidad en VMware vCenter Server.
6. Monitorear el rendimiento de vCenter, ESXi y máquinas virtuales.

5.2.2 Temario de la Capacitación

1. Introducción al Curso
2. Operaciones con Máquinas Virtuales
   - Administración de VMware Tools Repository.
   - Soluciones de respaldo y restauración de VMs.
   - Visualización de configuración de vSphere Replication y Site Recovery.
3. Gestión de Clústeres en vSphere
   - Visualización y administración de Resource Pools.
   - Funcionamiento de vCLS (vSphere Cluster Services).
4. Administración de vCenter y ESXi
   - Programación de respaldos de vCenter.
   - Visualización de alta disponibilidad en vCenter.
   - Uso de Host Profiles para la gestión de ESXi.
5. Monitoreo en vSphere
   - Factores clave que afectan el rendimiento de VMs.
   - Uso de herramientas de vCenter para análisis de recursos.
6. Seguridad y Control de Acceso
   - Estrategias de seguridad en vCenter, ESXi y VMs.

5.3 HPE ProLiant Gen11 Server Management with iLO 6

La capacitación de HPE ProLiant Gen11 Server Management with iLO 6 está diseñado para administradores e ingenieros que necesitan aprender a configurar, actualizar, monitorear y gestionar servidores HPE ProLiant Gen11 utilizando herramientas de administración embebidas como Integrated Lights-Out (iLO) 6.

Esta capacitación cubre desde la configuración inicial del hardware hasta la supervisión avanzada y actualización del firmware, proporcionando un enfoque integral para la gestión eficiente de servidores HPE en entornos empresariales.

Metodología
La capacitación combina teoría con ejemplos prácticos en un entorno real. Se utilizan los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicación detallada de conceptos clave.
- ✓ Ejemplos prácticos: Guía y muestra en vivo de servidores y herramientas en tiempo real.
- ✓ Interacción en sesiones de preguntas y respuestas.
- ✓ Duración: un (1) día.

Incluye:

- ✓ Administración de servidores HPE ProLiant Gen11.
- ✓ Gestión de iLO 6 para monitoreo y administración remota.
- ✓ Métodos para actualización de firmware con SPP y SUM.
- ✓ Visualización de configuración de seguridad, rendimiento y energía.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

No Incluye:

- ✓ Implementaciones personalizadas.
- ✓ Configuración avanzada fuera del entorno estándar del curso.
- ✓ Material oficial, libros y/o guías de certificación.
- ✓ Refrigerio.
- ✓ Certificación oficial del fabricante.

5.3.1 Objetivos de la Capacitación

Al finalizar el curso, los participantes serán capaces de:

1. Diferenciar las características de los servidores HPE ProLiant Gen11 y sus opciones de hardware y software.
2. Operar herramientas de administración embebida como iLO 6, UEFI ROM, y Intelligent Provisioning.
3. Visualizar medidas de seguridad y monitoreo para optimizar el rendimiento y consumo energético.
4. Monitorear servidores utilizando la interfaz de iLO 6, comandos REST y herramientas en la nube.
5. Actualizar el firmware de los servidores utilizando Service Pack for ProLiant (SPP) y Smart Update Manager (SUM).
6. Diagnosticar y solucionar problemas utilizando herramientas como Active Health System (AHS) y UEFI Embedded Diagnostics.

5.3.2 Temario de la Capacitación

1. Introducción al Hardware de HPE ProLiant Gen11
   - Características de los servidores Gen11.
   - Opciones de hardware y software.
   - Seguridad, garantía y soporte.
2. Introducción a las Herramientas de Administración
   - Gestión embebida en HPE ProLiant.
   - Uso de iLO 6, UEFI ROM, Intelligent Provisioning y Active Health System.
   - Gestión basada en la nube y Baseboard Management Controller (BMC).
3. Administración con iLO 6
   - Acceso remoto y administración de servidores.
   - Configuración de seguridad y políticas de acceso.
   - Opciones de gestión de energía y temperatura.
4. Actualización del Servidor
   - Métodos de actualización de firmware.

- Uso de Service Pack for ProLiant (SPP) y Smart Update Manager (SUM).
- Procedimientos de actualización de iLO 6.

5. Monitoreo del Servidor
   - Uso de iLO 6 y herramientas de monitoreo.
   - Configuración de alertas y análisis de rendimiento.
   - Verificación de firmware y monitoreo con RESTful API.
6. Diagnóstico y Solución de Problemas
   - Herramientas de diagnóstico embebidas en UEFI e iLO.
   - Descarga y análisis de logs con Active Health System (AHS).
   - Indicadores LED y su interpretación.
7. Recursos y Soporte
   - Uso del HPE Support Center y My Software Center Dashboard.
   - Acceso a actualizaciones y materiales de soporte.
   - Pasos siguientes para continuar el aprendizaje.

6. Premisas y Entregables

- ✓ El Consorcio EMDOC se hace responsable de la entrega de todos los servicios de instalación y configuración de los equipos ofertados.
- ✓ El Consorcio EMDOC se hace responsable de la realización de las configuraciones, actualizaciones y mejoras de software necesarias para la integración de los nuevos equipos.
- ✓ Nuestra propuesta incluye todo el hardware, software y licenciamientos necesarios para la instalación y operación tal y como es requerido.
- ✓ Nuestra propuesta incluye soporte de tipo proactivo con SLA de atención 24x7x4 con una duración de cinco (5) años a partir de la fecha de aceptación por escrito por parte de la Junta Central Electoral y puesta en marcha de los equipos.
- ✓ Nuestra propuesta incluye equipos nuevos no reconstruidos.
- ✓ Nuestra propuesta incluye plan de trabajo detallado en la propuesta técnica en el cual se especifica de forma clara todos los pasos a ejecutar durante el proceso de implementación de los equipos ofertados.
- ✓ Nuestra propuesta incluye proveer, instalar y configurar todos los equipos, hardware y licencias con las características técnicas mencionadas según la tabla de referencias. La solución propuesta está integrada y certificada de fábrica en todos sus componentes como un solo producto según cada lote.
- ✓ Nuestra propuesta incluye la entrega de todos los equipos en completa operación, a satisfacción de la entidad, con todos los componentes solicitados incluidos.
- ✓ Se incluyen todas las hojas técnicas (DataSheets) de los propuestos ofertados, así como el link correspondiente del fabricante.
- ✓ Nuestra propuesta incluye equipos nuevos de fábrica, no se incluyen equipos reemplazos o remanufacturados.
- ✓ Se incluyen cartas del fabricante en la cual el Consorcio EMDOC a través de los miembros del consorcio cuenta con las debidas autorizaciones a ofrecer los bienes y servicios presentados en nuestra oferta.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

- ✓ Se incluye carta del fabricante en la cual se indica que todos los equipos ofertados son nuevos, no usados, no remanufactorados, ni reparados y que los mismos no se encuentran descontinuados ni anunciados fuera de vida.
- ✓ Nuestra propuesta incluye la asignación de un gerente de proyectos certificado PMP dedicado 100% de su tiempo a la implantación de todas las soluciones ofertadas en este lote durante todo el tiempo que sea necesario y requerido por la institución hasta la conclusión y recepción del proyecto. Este Gerente de proyecto es empleado fijo de uno de los miembros del Consorcio EMDOC con más de 6 meses en la empresa.